Physical Unclonable Functions for IoT Security

Muhammad Naveed Aman
National University of Singapore
Singapore 117583
elemna@nus.edu.sg

Kee Chaing Chua
National University of Singapore
Singapore 117583
@nus.edu.sg

Biplab Sikdar
National University of Singapore
Singapore 117583
bsikdar@nus.edu.sg

ABSTRACT

Keywords

IoT security, Physical unclonable functions

1. INTRODUCTION

Traditionally security for the Internet has been provided by classical cryptography. These security primitives and techniques were designed with an implied assumption of physically well protected devices. However, with the introduction of Internet of Things (IoT), wireless sensor networks (WSNs), and portable computing, security needs to cover a much wider spectrum of problems. One of the important tasks is how to provide fool proof security to physically unprotected devices with limited resources. Most of the devices in IoT are physically unprotected and not only are they easily accessible but may even reside in hostile environments.

IoT devices have outnumbers human beings by a ratio of 1.5 to 1 [1]. Although the realization of IoT systems includes many constraints including power, cost, lifetime, and energy. However, the most challenging requirement is considered to be security. It is of utmost importance to make IoT systems secure because security in IoT is directly connected to human safety. Given the huge number of IoT devices, simple nature, and the fact that they are not operated by a human makes the task of designing security protocols for them extremely difficult. While existing security primitives may be sufficient for the Internet but they are not suitable for IoT. Modern security protocols need to be immune to physical and side channel attacks in addition to providing anonymity, privacy, and trust. Moreover, security protocols for the IoT must also have very low computational, memory, and power requirements.

Biometric systems can verify the identity of human beings in a very effective manner due to the uniqueness of these features. Inspired by biometrics, physical unclonable functions (PUFs) provide a unique way to identify integrated circuits (ICs). This idea was first put forward by [2]. PUFs exploit the inherent variability in integrated circuit (IC) manufacturing to implement challenge-response functions whose output depends on the input and the physical micro-structure of the device.

Some of the critical operations that IoT devices need to perform include authentication, data integrity, access control, privacy, and digital forgetting [3, 4, 5]. Contemporary techniques use digital signatures and encryption with a secret key to enable the above security operations. However, these techniques are not suitable for IoT devices due to the following two reasons. Firstly, the low cost and simple nature of IoT devices may not be enough to provide the processing power required for most digital signature and encryption schemes. Secondly, it may not be feasible to manage secrets in IoT devices. Secrets are usually stored in non-volatile memories or battery-backed RAMs which can be read using different kind attacks such as invasive or semi-invasive attacks [6]. Moreover, providing high level of physical security to IoT devices using tamper-sensing circuitry may be very expensive in terms of cost as well as energy.

From the discussion above, it becomes clear that the current security primitives are not suitable for providing security in IoT systems. PUFs on the other hand, due to their unique characteristics, may provide an efficient, and low cost solution to security in IoT systems. PUFs may be used to provide security in IoT systems without the need to store secrets in the devices. Moreover, the variations in the physical factors during the fabrication process of ICs make it practically impossible to replicate the micro-structure, making PUFs unique at a device level.

In this paper we present several security challenges in IoT systems and propose PUFs to be used to solve these issues. The rest of the paper is organized as follows. Section 2 presents a brief intrduction to PUFs. Section 3 discusses the different security challenges in IoT systems and how PUFs can be used to efficiently solve these problems. In Section 4 we present a protocol for mutual authentication in IoT systems. Finally, we conclude in Section 5.

2. INTRODUCTION TO PHYSICALL UNCLONABLE FUNCTIONS

[7] describe a PUF as "A Physical Unclonable Function (PUF) is a function that maps a set of challenges to a set of responses based on an intractably complex physical system".

3. SECURITY CHALLENGES OF THE IOT AND PUFS

DOI: 10.1145/1235

In this section we describe the unique security challenges in IoT systems which can be solved efficiently using PUFs. The simple and low cost nature of PUFs makes them a prime target for adversaries. The major security challenges for IoT include authentication, self trust, access control, data integrity, low cost energy aware protocols; and side channel, physical, and cloning attacks. Some of these problems can be solved efficiently using PUFs as discussed as follows:

3.1 Authentication

IoT systems are expected to encompass billions of devices. Each device should be able to authenticate itself to the network before sending or receiving data. As most of the IoT devices will not have any human operator sitting behind them, each IoT device must be equipped with a way to identify and authenticate itself. The contemporary techniques for authentication require some kind of secret credentials to be stored in the device's memory. However, these techniques are not suitable for physically unprotected devices like the diverse devices that are part of an IoT system. An adversary may use different type of physical attacks to compromise the security of the whole system. The use of PUFs serves two purposes: firstly, they provide a mechanism for volatile secrets [7] i.e., the secret does not exist in digital form instead it is embedded into the micro-structure of the PUF IC. Secondly, each PUF is unique and in turn can be used to provide a unique identity to each IoT device.

3.2 Self Trust

Self trust, a conceptually new security task, enables a user to trust an IoT device. This enables a user to trust that the data received is indeed collected by the specific device at the stated time and location. Several works on using hardware security primitives for trust in IoT have been presented [3]. However, these techniques need to be further optimized in terms of energy and cost. Given the low energy footprint of PUFs, they can form a suitable choice for the realization of self trust in IoT systems.

3.3 Protection against Physical and Cloning Attacks

An adversary may try to impersonate itself as an authentic IoT device by cloning another IoT device. As discussed previously, IoT systems are deployed out in the open. An adversary may easily access an IoT device and try to clone it by extracting secrets from the device. However, the use of PUFs makes this type of attacks extremely difficult for an adversary. Launching a cloning attack on PUFs means creating an exact copy of the PUF IC which in turn translates into using invasive techniques to measure the PUF delays accurately. It has been shown in [8, 9], that PUFs can be used effectively for hardware obfuscation. This shows that by using PUFs IoT devices can be made secure against physical and cloning attacks.

3.4 Protection against Side Channel Attacks

The easy access to IoT devices for an adversary opens doors for side channel attacks. The prominent attacks in this category include timing attacks, power monitoring attacks, electromagnetic attacks and differential fault analysis. Timing attacks usually involves statistical analysis of the timing required to perform cryptographic operations by a CPU and there by determining the secret key. However, PUFs use a challenge response mechanism instead of secret keys. It may be possible to measure the computation time of a CPU but it may not be possible to accurately measure the timing delays of an IC. Moreover, PUFs are considered isochronous and therefore not susceptible to timing attacks.

Power monitoring attacks depend on monitoring the power consumption during computations. The authors of [10] have shown a power side-channel attack on PUFs using a data analysis algorithm. They have shown that by using the power consumption the number of zeros and ones stored in the latches of an arbiter PUF. However, by designing the PUF in such a way that the number of zeros and ones in the latches is constant we can make PUFs secure against these type of attacks.

Performing an electromagnetic attack is practically more complex than a power monitoring attack. It requires deep knowledge of frequency domain and high frequency measurement equipment. Similar to power analysis attacks, by reducing the fluctuations in current we can make the PUF secure against electromagnetic attacks as well.

Differential fault analysis is carried out by introducing faults i.e., abnormal environmental conditions, into security hardware to reveal their internal state. Some types of PUFs are extremely sensitive to the external environment e.g., the delay-based PUF is very sensitive to temperature and voltage variations. An adversary may try to launch a differential fault analysis on these types of PUFs which will make them unstable. These type of attacks usually use the physical corruption of data, however, as there is no physical data inside the PUF these type of attacks may not produce any fruitful results.

3.5 Man-in-the-middle Attacks

An adversary may try to reuse an older challenge if somehow he/she gets one of the CRPs for a PUF. He/she may try to exploit this CRP by re-using it for authentication or other security operations. It is desired that a CRP is never reused. The class of reconfigurable PUFs can be an interesting area of future research for this purpose. PUFs can be made reconfigurable after each CRP, this will make the system immune to replay and man-in-the-middle attacks.

3.6 Low Cost Energy Aware Protocols

PUFs can be ultra fast, have ultra low energy consumption, and very small silicon footprint. These characteristics make them an ideal choice for the realization of ultra fast protocols having very low energy requirements. It is very important that any security protocol designed for the IoT should be able to support real time applications with minimum energy requirements.

4. PROPOSED PUF BASED MUTUAL AUTHENTICATION PROTOCOL

4.1 Network Model, Assumptions, and Notations

In our network model, IoT devices equipped with PUFs are connected to a server in a data center through the Internet as shown in Figure 1. Assumptions for the proposed protocol and network model are as follows:

a. The PUF and the device's microcontroller are considered to be on the same chip and inseparable. It is not possible

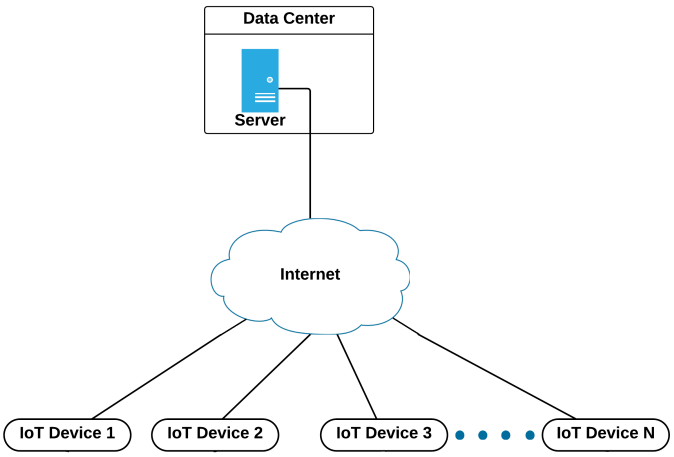

Figure 1: Network Model

to remove the PUF or tamper with the communication between the microcontroller and PUF.

b. IoT devices are constrained by their resources, while that data center has no such limitation.

c. IoT devices are physically unprotected and easily accessible by an adversary.

d. An adversary can eavesdrop, modify, inject, and replay messages.

Moreover, let us denote the ID of an IoT device, XOR operation, Hash of X, challenge for the i'th iteration, and response of a PUF to input C^i with ID_i, $\oplus$, $H(X)$, C^i, and R^i respectively.

4.2 Proposed Protocol

In this section we describe a low cost protocol for authentication in IoT systems. The proposed protocol is shown in Figure 2. We assume that before this protocol is run the server has a secure way to obtain an initial challenge response pair (CRP) in offline mode. The steps of the protocol are as follows:

1. The IoT device sends its ID_i and a random number $nonce_i$ to the server.

2. The server searches its memory for ID_i and retrieves the respective CRP (C^i, R^i) for the PUF of this IoT device. If ID_i is not found in its memory the authentication request is rejected. The server then generates a secret random number N_A and uses it to hide R^i in message 2 of the protocol. The server uses a message authentication code (MAC) for data integrity.

3. The IoT device uses its PUF to get R^i from C^i. It then uses R^i to obtain N_A and then verifies the freshness and integrity of the message using the received MAC. The IoT device then generates a new challenge C^{i+1} using N_A and N_B. The new challenge is input to the device's PUF to obtain the new secret response R^{i+1}. N_B and R^{i+1} are sent securely to the server using N_A as shown in message 3. The IoT device also sends a MAC in message 3.

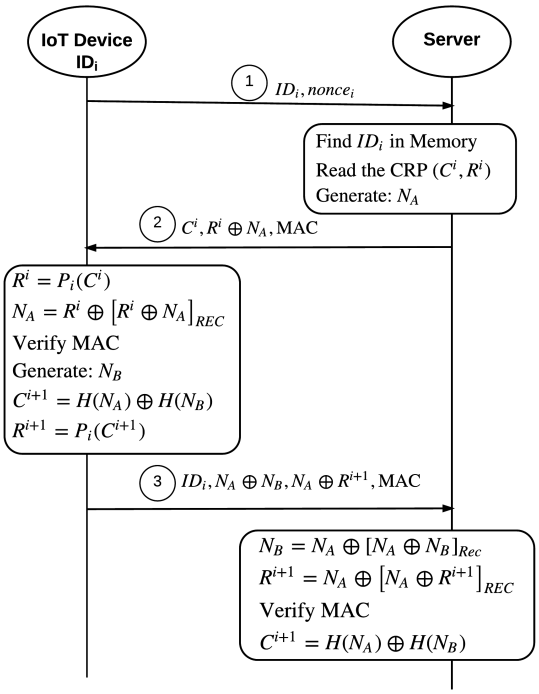

Figure 2: Proposed Mutual Authentication Protocol

4. The server calculates N_B and R^{i+1} using its secret N_A, and verifies the message using the MAC. The server then uses N_A and N_B to construct the new challenge and saves the new CRP (C^{i+1}, R^{i+1}) against ID_i in its memory.

In the above steps if at any step the MAC fails verification, the authentication request is terminated. Please note that the MACs do not use any secret key stored in the device before the protocol is run, instead they use the secret random numbers N_A and N_B generated during the protocol. At the end of the protocol the IoT device and server delete all temporary variables including N_A, N_B, $nonce_i$, C^{i+1}, and R^{i+1} from their memories. The secret numbers N_A and N_B can also be used to establish a secret shared key e.g., $H(N_A \parallel N_B)$ can be used as a shared symmetric key between the IoT device and server for further communication.

4.3 Security Analysis

The simple and low cost nature of IoT device make them vulnerable to different kind of attacks as discussed in Section 3. However, with the use of PUF our proposed protocol is secure against these attacks as described as follows:

1. The proposed protocol is immune to cloning or impersonation attacks because a PUF cannot be reproduced and each PUF will have its own unique CRP.

2. The proposed protocol is secure against physical attacks mainly due to two reasons. Firstly, devices do not store any secrets in their memory. Secondly, as the device's microcontroller and PUF are on the same chip, the communication between them is considered

to be secure [11]. This shows that even if a device is physically available to an adversary, he/she cannot extract any secrets from the device.

3. An adversary may try to replay older messages. However, the proposed protocol uses a new random number each time in each of its messages. For example, messages 1, 2, and 3 each have a new random number $nonce_i$, N_A, and N_B respectively. Therefore, the proposed protocol is safe against replay attacks.

4. An adversary may attempt to modify the contents of the different messages. However, the use of MACs with new secrets every new run of the protocol makes the proposed protocol secure against these type of attacks.

5. To construct valid data an adversary needs to know R^i, N_A or N_B. An adversary cannot obtain these secrets with any of the other attacks including eavesdropping, man-in-the middle attack, spoofing attacks, and interleaving attacks etc.

4.4 Performance Analysis

In this section we show that the proposed protocol is very efficient in terms of computation, communication, and communication overhead.

If we represent the number of hash operations, number of exclusive-or operations, and number of MACs by N_H, $N_\oplus$, and N_{MAC} respectively. Then an IoT device requires $2N_H + 4N_\oplus + 1N_{MAC}$ operations while the server requires $2N_H + 4N_\oplus + 1N_{MAC}$ operations. This shows that the proposed protocol requires very low processing power to perform authentication in comparison to other contemporary authentication schemes. For example, the computational cost of an RSA digital signature is given by $\frac{3}{2}nM(n)$ which for a 1024 bit key translates into more than 1500 operations. The low computational burden translates into low energy requirements as well.

The proposed protocol also has very low communication overhead. If we assume the size of the output of the PUF and a MAC to be 128 bits, the maximum size of any message in our protocol is not more than 64 bytes. This is very low as compared to other signature based schemes e.g., the size of an RSA signature is typically in the range of 128 to 256 bytes. Moreover, the number of message are also equal to a two way handshake which is very efficient.

In addition to low computation and low communication overhead, the proposed protocol also has very low storage requirements. Many PUF based protocols [7, 12] require the server to store a large number of CRPs in its memory. However, given the large number of IoT devices this approach does not scale well. On the other hand our proposed protocol requires the server to store only one CRP for each IoT device. Moreover, each IoT device does not need to store anything except its ID.

The above discussion shows that the use of PUF not only provides fool proof security but can also result in very efficient realizations of security protocols for IoT systems.

5. CONCLUSIONS

The existing encryption based security protocols are not suitable for IoT systems. The simple, low cost, and divers nature of IoT devices make them vulnerable to physical, side channel, and cloning attacks. PUFs provide an innovative and unique way to secure the IoT from these type of attacks. PUFs can be used to provide efficient and effective security solutions for IoT systems. A PUF based mutual authentication protocol is presented. The security and performance analysis of the proposed protocol shows that PUFs can be used to realize security protocols for IoT devices.

6. REFERENCES

[1] *The Internet of Things Reference Model,* CISCO, 2014.

[2] K. Lofstrom, W. R. Daasch, and D. Taylor. "IC identification circuit using device mismatch,"*Proceedings of ISSCC 2000,* February 2000.

[3] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT Systems: Design Challenges and Opportunities,"*Proceedings of IEEE/ACM ICCAD,* pp. 417-423, San Jose, CA, November 2014.

[4] *Security in the Internet of Things*, Wind River, January 2015.

[5] G. Woo, P. Kheradpour, D. Shen and D. Katabi, "Gartner Says the Internet of Things will Transform the Data Center," Gartner, March 2014.

[6] S. P. Skorobogatov. "Semi-invasive attacks - a new approach to hardware security analysis," *Technical Report UCAM-CL-TR-630,* University of Cambridge Computer Laboratory, April 2005.

[7] G. E. Suh, and S. Devadas "Pysical Unclonable Functions for Device Authentication and Secret Key Generation," *Proceedings of IEEE/ACM DAC,* pp. 9-14, San Diego, CA, June 2007.

[8] J. B. Wendt and M. Potkonjak, "Hardware obfuscation using PUFbased logic," *International Conference on Computer-Aided Design (ICCAD),* pp. 1âĂŞ8, 2014.

[9] T. Xu, J. B. Wendt, and M. Potkonjak, "Secure remote sensing and communication using digital PUFs," *Symposium on Architectures for Networking and Communications Systems (ANCS),* pp. 1âĂŞ12, 2014.

[10] A. Mahmoud et. al. "Combined Modeling and Side Channel Attacks on Strong PUFs," *IACR Cryptology ePrint Archive,* no. 632, 2013.

[11] S. Guilley, and R. Pacalet, "SoCs security: a war against side-channels", *Annals of Telecommunications,* Vol. 59, no. 7, pp 998-1009, 2004.

[12] H. Ghaith, O. Erdinc, and S. Berk, "A Tamper-Proof and Lightweight Authentication Scheme", *Pervasive Mobile Computing,* Vol.4, no.6, pp. 807-818, 2008.